-2-

IN THE CLAIMS

Amended claims follow:

- (Currently Amended) A method for network-based scanning for potentially 1. malicious content, comprising:
- monitoring network communications over a network; (a)

SVIPG

- identifying potentially malicious content in the network communications; (b)
- quarantining the potentially malicious content of the network communications; (¢)
- executing a pattern for testing the potentially malicious content network (d) communications for malicious code; and
- (e) conditionally delivering the network communications over the network based on the testing: wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.
- 2. (Original) The method as recited in claim 1, further comprising scanning the network communications for known malicious content.
- (Original) The method as recited in claim 1, wherein the malicious content 3. includes a mass-mailer virus.
- 4. (Original) The method as recited in claim 1, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.
- 5. (Original) The method as recited in claim 1, wherein the network communications include electronic mail messages.

- (Original) The method as recited in claim 5, wherein an electronic mail message 6. is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.
- 7. (Cancelled)

Jul 07 05 09:50a

- (Currently Amended) The method as recited in claim 1, further comprising 8. cleaning the potentially malicious content if malicious code is found, which is[for] disabling [the]of malicious code.
- (Currently Amended) A computer program product embodied on a computer 9. readable medium for network-based scanning for potentially malicious content, comprising:
- computer code that monitors network communications over a network; (a)
- computer code that identifies potentially malicious content in the network (b) communications;
- computer code that quarantines the potentially malicious content of the network (c) communications;
- computer code that executes a pattern for testing the potentially malicious content (d) network communications for malicious code; and
- computer code that conditionally delivers the network communications over the (e) network based on the testing; wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.
- (Currently Amended) A system for network-based scanning for potentially 10. malicious content, comprising:
- logic that monitors network communications over a network; (a)
- logic that identifies potentially malicious content in the network communications; (b)

- (c) logic that quarantines the potentially malicious content of the network communications;
- (d) logic that executes a pattern for testing the potentially malicious content network communications for malicious code; and
- (e) logic that conditionally delivers the network communications over the network based on the testing;

 wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.
- 11. (Currently Amended) A method for network-based scanning for potentially malicious content, comprising:
- (a) monitoring network communications over a network;
- (b) identifying potentially malicious content in the network communications;
- quarantining the potentially malicious content of the network communications;
 and
- (d) delivering the network communications over the network after a predetermined delay;
 wherein the delay is for allowing quarantining of the potentially malicious content until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.
- 12. (Original) The method as recited in claim 11, further comprising scanning the network communications for known malicious content.
- 13. (Original) The method as recited in claim 11, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.
- 14. (Original) The method as recited in claim 11, wherein the network communications include electronic mail messages.

- 15. (Original) The method as recited in claim 14, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.
- 16. (Cancelled)
- 17. (Currently Amended) A method for network-based scanning for potentially malicious content, comprising:
- (a) monitoring network communications over a network;
- (b) identifying potentially malicious content in the network communications;
- (c) quarantining the potentially malicious content of the network communications in a quarantine; and
- (d) delivering the network communications from the quarantine over the network in response to a request from a user;
 wherein it is determined whether the user is authorized, and the network communications are delivered only if the user is determined to be authorized.
- 18. (Original) The method as recited in claim 17, wherein the user is an intended recipient of the quarantined network communications.
- 19. (Original) The method as recited in claim 17, further comprising scanning the network communications for known malicious content.
- 20. (Original) The method as recited in claim 17, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.
- 21. (Original) The method as recited in claim 17, wherein the network communications include electronic mail messages.

Jul 07 05 09:50a

- 22. (Original) The method as recited in claim 21, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.
- (Currently Amended) A method for network-based scanning for potentially 23. malicious content, comprising:
- monitoring incoming and outgoing network communications over a network at a (a) gateway;
- scanning the network communications for known malicious content; (b)
- identifying potentially malicious content in the network communications; (c)
- (d) wherein content is identified as potentially malicious when a number of identical instances of the content in the network communications passing through the network for a given period of time is greater than a predetermined value;
- wherein the network communications include electronic mail messages, wherein (e) an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line passing through the network for a given period of time is greater than a predetermined value;
- (f) quarantining the potentially malicious content of the network communications;
- delivering the network communications over the network upon occurrence of the (g) first of:
 - scanning the potentially malicious content with a malicious code (i) detection file received after the potentially malicious content is received;
 - (ii) upon receiving a user request;
 - upon passage of a predetermined amount of time; (iii)
- (h) notifying an intended recipient of the potentially malicious content that the potentially malicious content has been quarantined;
- notifying a sender of the potentially malicious content that the potentially (i) malicious content has been quarantined; and
- (j) cleaning the potentially malicious content if malicious code is found, which is for] disabling [the]of malicious code.

Jul 07 05 09:50a

- 24. (New) The method as recited in claim 1, wherein the potentially malicious content is identified utilizing heuristics.
- 25. (New) The method as recited in claim 24, wherein the heuristics include generating a histogram of content that has been sent over the network during a period of time and analyzing the histogram to determine whether a number of copies of the potentially malicious content that have been sent over the network during the period of time exceed a predetermined value.
- 26. (New) The method as recited in claim 1, wherein the quarantining includes containing the potentially malicious content and preventing the potentially malicious content from creating damage.
- (New) The method as recited in claim 1, wherein when multiple recipients are to receive a copy of the potentially malicious content over the network, a single copy of the potentially malicious content is quarantined and each of the recipients is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients.
- 28. (New) The method as recited in claim I, wherein an intended recipient of the network communications is notified that the potentially malicious content is quarantined.